# STATE OF SOUTH DAKOTA
# CONSULTING CONTRACT

This Agreement made and entered into by and between the South Dakota Bureau of Finance and Management, a state agency, of 500 East Capitol Avenue, Pierre, South Dakota 57501, (hereinafter the "State") and Guidehouse Inc., a Delaware Corporation with offices at 1800 Tysons Blvd, 7th Floor, McLean, VA, 22102 (hereinafter the "Consultant").

1. The Consultant is hereby retained to provide support for the State's expenditure of funds received pursuant to section 5001 of the Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, div. A, Title V (Mar. 27, 2020) ("CRF Funds"). Consultant will more specifically perform those services outlined in one or more Task Orders the State may issue to the Consultant pursuant to this Agreement. Each Task Order shall incorporate a statement of work further detailing the specific activities to be performed, applicable deliverables and timeline, and any specific arrangements agreed upon by the parties relating to that task. Each individual Task Order shall be attached hereto as a supplement to Exhibit A and hereby incorporated by reference. Except as otherwise provided for herein, in the event of a conflict between a Task Order and the terms of this Agreement, the language of this Agreement shall control.

2. This Agreement shall be effective beginning October 1, 2020 and shall end on March 30, 2021, unless sooner terminated pursuant to the terms hereof.

3. The Consultant will not use State equipment, supplies or facilities. The Consultant will provide the State with its Employer Identification Number and Federal Tax Identification Number upon execution of this Agreement.

4. The State will make payment for services upon forty-five (45) days receipt of an undisputed invoice. The TOTAL CONTRACT AMOUNT is an amount not to exceed **$6,000,000.00.** Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Consultant will invoice on a monthly basis for time incurred by Consultant's professionals based on the hourly rates set forth below. In the event a Task Order sets forth a different schedule of hourly rates for Consultant's professionals, the rates provided in that Task Order shall apply only to the work performed under that Task Order. Payment will be made consistent with SDCL ch. 5-26.

| Role | Rate/hour |
|---|---|
| Engagement Partner | $390.00 |
| Subject Matter Expert | $310.00 |
| Program Manager/Director | $280.00 |
| Salesforce Certified Developer | $280.00 |
| Project Manager/Manager | $265.00 |
| Senior Consultant | $185.00 |
| Consultant | $145.00 |

| | |
|---|---|
| Associate III | $125.00 |
| Associate II | $110.00 |
| Analyst I | $75.00 |
| Support Analyst | $50.00 |

In addition to hourly rates for time incurred, the State will reimburse the Consultant for out-of-pocket expenses related to transportation and lodging. Transportation shall be in the class and fare available that is most economical to the State. Lodging shall be in regular, non-suite rooms. The State will also reimburse the Consultant a per diem fee of $50 for meals for each travel day per person related to this Agreement.

5. Indemnification

A. The Consultant agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against third-party actions, suits, damages, liability or other proceedings for (a) damage to real or tangible property, (b) death or bodily injury, or (c) assessment of repayment, penalties, and interest made against the State by the U.S. Treasury Department arising directly as the result of performing professional services hereunder. The Consultant also agrees to indemnify and hold the State of South Dakota, its officers, agents, and employees, harmless from and against third-party actions, suits, damages, liability, or other proceedings that may arise as a result of a claim alleging that any report, record, program, drawing, written materials, intellectual property or other work product provided by Consultant infringes or misappropriates a U.S. patent, U.S. copyright, U.S. trademark, or U.S. trade secret of a third party. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

B. Except to the extent finally determined to have resulted from Consultant's gross negligence or intentional misconduct hereunder, Consultant's aggregate liability for all claims, losses, liability, or damages in connection with this Agreement or its subject matter, whether as a result of breach of contract, tort (including negligence), or otherwise, regardless of the theory of liability asserted, is limited to five hundred percent (500%) of the total amount of fees paid to Consultant under the applicable Task Order. In addition, Consultant will not be liable in any event for lost profits, consequential, indirect, punitive, exemplary, or special damages. Consultant shall also have no liability to the State arising from or relating to any third-party hardware, software, information, or materials selected or supplied by the State. This paragraph 5.B. shall not apply to any third-party damages or liabilities, as finally determined by a court of competent jurisdiction that may arise directly as a result of a claim alleging that any report, record, program, drawing, written materials, intellectual property or other work product provided by Consultant infringes or misappropriates a U.S. patent, U.S. copyright, U.S. trademark, or U.S. trade secret of a third party.

6. The Consultant, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:

The Consultant shall maintain occurrence-based commercial general liability insurance or equivalent form with a limit of not less than $1,000,000.00 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than seven times the occurrence limit.

B. Professional Indemnity Insurance or Miscellaneous Professional Liability Insurance:

The Consultant agrees to procure and maintain professional indemnity insurance or miscellaneous professional liability insurance with a limit of $1,000,000.00 per claim and $5,000,000.00 in the aggregate.

C. Business Automobile Liability Insurance:

The Consultant shall maintain business automobile liability insurance or equivalent form with a limit of $1,000,000.00 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

D. Worker's Compensation Insurance:

The Consultant shall procure and maintain workers' compensation and employers' liability insurance as required by applicable law.

E. Cyber Liability Insurance:

The Consultant shall maintain cyber liability insurance with liability limits in the amount of $1,000,000.00 per claim to protect any and all State data the Consultant receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Consultant employees, whether the device is owned by the employee or the Consultant. If the Consultant has a contract with a third-party to host any State data the Consultant receives as part of the project under this agreement, then the Consultant shall include a requirement for cyber liability insurance as part of the contract between the Consultant and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-part Consultant. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and

regulatory fines. The insurance will stay in effect for six (6) years after the work covered by this agreement is completed.

The Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. In the event of a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State only in the event a policy is not replaced with a policy that meets the insurance requirements of this section or there is a lapse in coverage. Consultant shall provide a new or renewal certificate of insurance showing continuous coverage in the amounts required. In addition, in the event of a change in the company from which the insurance is obtained, Consultant shall provide the State with the name of the new insurer and the insurer's National Association of Insurance Commissioners (NAIC) code.

7. While performing services hereunder, the Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

8. Consultant agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Consultant or the State to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.

9. This Agreement may be terminated by the State upon thirty (30) days written notice. This Agreement may be terminated by the Consultant upon ninety (90) days written notice. In the event the Consultant breaches any of the terms or conditions of this Agreement, the State may terminate this Agreement at any time with written notice; provided the State grants the Consultant a reasonable opportunity to cure. If termination for such a default is effected by the State, any payments due to Consultant at the time of termination may be adjusted to cover any additional costs to the State due to Consultant's default. Upon termination, the State may take over the work and may award another party an agreement to complete the work under this Agreement. If, after the State terminates for a default by Consultant, it is determined that Consultant was not at fault, the State will pay Consultant for eligible services rendered and expenses incurred up to the date of termination.

10. This Agreement depends upon the continued availability of federal funds for this purpose. If for any reason funds become unavailable by operation of law or federal funds reductions, this Agreement will be terminated by the State. Termination for

any of these reasons is not a default by the State nor does it give rise to a claim against the State.

11. This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

12. This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, exclusive of its choice of law provisions. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

13. The Consultant will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

14. The Consultant agrees to abide by all applicable provisions of the following assurances:

(a)Title VI of the Civil Rights Act of 1964 (P.L. 88-352);
(b)Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§ 1681-1683, and 1685-1686);
(c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794) and the Americans with Disabilities Act of 1990 (42 USC § 12101, et seq.; PL 101-336);
(d) the Age Discrimination Act of 1975, as amended (42U.S.C. §§ 6101-6107);
(e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended;
(f) the comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970(P.L. 91-616), as amended;
(g) §§ 523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§ 290 dd-3 and 290 ee-3), as amended;
(h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§ 3601 et seq);
(i) the Civil Rights Restoration Act of 1987;
(j) the Drug-free Workplace Act of 1988 (41 U.S.C. 702);
(k) the Buy America Act (49 U.S.C. 5323 (j));
(l) the Hatch Act (5 U.S.C. §§ 1501-1508 and 7324-7328);
(m) Executive Order 11246 Equal Employment Opportunity
(n) Contract Work Hours and Safety Standards Act (40 U.S.C. §§ 3701-3708).
(o) Clean Air Act (42 U.S.C. §§ 7401-7671q) and the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1387).
(p) Debarment and Suspension (Executive Orders 12549 and 12689).
(q) Byrd Anti-Lobbying Amendment (31 U.S.C. § 1352).

15. The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the project, including records and

documents regarding applications, determination for eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for six years following termination of this Agreement. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State, not to exceed seven (7) years. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers, or documents related to services rendered under this Agreement.

16. The Consultant certifies that neither Consultant nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. The Consultant further agrees that it will immediately notify the State if during the term of this Agreement Consultant or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

17. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state, and local laws, regulations, ordinances, guideline, permits, and requirements, in particular all guidance issued by the U.S. Department of Treasury with respect to CRF Funds, and will adopt such review and inspection procedures as are necessary to assure such compliance. After providing notice to the State, the Consultant may draw from the resources of and/or subcontract to (i) its subsidiaries and affiliates in connection with the provision of professional services under this Agreement; and/or (ii) third-party contractors within or outside the United States for internal, administrative, and/or regulatory compliance purposes. With the prior written consent of the State, the Consultant may draw from the resources of and/or subcontract to other third-party contractors for the performance of professional services under this Agreement. The State agrees that the Consultant may provide information it receives in connection with this Agreement to its subcontractors and for compliance with the other terms and conditions of this Agreement. However, the Consultant will be ultimately responsible for the provision of professional services, including those performed by any subcontractors, for the protection of any confidential information provided to its subcontractors, and for compliance with the other terms and conditions of this Agreement. The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, and to provide insurance coverage in a manner consistent with this Agreement.

18. Pursuant to Executive Order 2020-01, for contractors, vendors, suppliers, or subcontracts with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by signing this contract the Consultant certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to

the subject matter of the contract, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to terminate this contract. The Consultant further agrees to provide immediate written notice to the State if during the term of the contract it no longer complies with this certification, and agrees such noncompliance may be grounds for contract termination.

19. Any notice or other communication required under this Agreement shall be in writing and sent to the addresses set forth above. Notices shall be given by and to **Liza Clark** on behalf of the State, and by and to **Jeff Bankowski** on behalf of the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

20. In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof. Failure to strictly enforce any provision of this Agreement shall not constitute a waiver of any provision, right or responsibility contained herein.

21. All other prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

22. The parties expressly agree the terms of paragraphs 5, 12, and 15 survive termination of this Agreement.

23. Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software and services; telecommunication equipment, software and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions and other units of state government. BIT requires the contract provisions which are attached to this Agreement as Exhibit B and hereby incorporated into this Agreement by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only Exhibit B of this agreement. Before renewal of this Agreement, BIT must review and approve Exhibit B as still being current. BIT's evaluation of Exhibit B will be based on changes in the IT security or regulatory requirements. Changes to Exhibit B must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be

provided to the Consultant with the understanding that the Consultant will adhere to the most current State IT security policies.

24. State acknowledges that it has complied with the requirements of SDCL 5-18D-17 to 5-18D-22 inclusive. This Agreement is exempt from RFP requirements pursuant to SDCL 5-18A-9 and 5-18D-21(2).

In Witness Whereof, the parties signify their agreement effective the date above first written by the signatures affixed below.

STATE

BY: Liza Clark
Liza Clark

Commissioner,
Bureau of Finance and Management

10/9/2020
Date

CONSULTANT

BY: Jeff Bankowski

Print Name: Jeff Bankowski

Partner

Title

10/9/2020
Date

Jeffrey Clines
Jeffrey Clines (Oct 9, 2020 15:18 MDT)

Jeffrey Clines
Commissioner,
SD Bureau of Information and Telecommunications

10/09/2020
DATE

**Exhibit B**
**Technical Provisions**

1. DATA PROTECTION

Protection of personal privacy and data shall be an integral part of the business activities of the Consultant to ensure there is no inappropriate or unauthorized use of State's data at any time. To this end, the Consultant shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

A. The Consultant shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Heath Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Consultant applies to its own non-public data.

B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Consultant or any party related to the Consultant for subsequent use in any transaction that does not include the State.

C. The Consultant will not use such data for the Consultant's own benefit and, in particular will not engage in data mining of State's data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

2. NON-DISCLOSURE AND SEPARATION OF DUTIES

The Consultant shall enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State data or the hardware that State data resides on. The Consultant will limit staff knowledge to those staff who duties that require them to have access to the State's data or the hardware the State's data resides on.

3. RIGHTS AND LICENSE IN AND TO STATE DATA

The parties agree that between them, all rights including all intellectual property rights in and to State's data shall remain the exclusive property of the State, and that the Consultant has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

4. LEGAL REQUESTS FOR DATA

Except as otherwise expressly prohibited by law, the Consultant will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Consultant seeking State data maintained by the Consultant;

B. Consult with the State regarding its response;

C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and

D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

5. EDISCOVERY

The Consultant shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Consultant shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

6. ACCESS ATTEMPTS

All access attempts, whether failed or successful, to any Consultant system connected to the hosted system at salesforce.com which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Consultant. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 1 year in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

7. PASSWORD POLICIES

Password policies for all Consultant employees will be documented annually and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced.

## 8. SUSPENSION OF SERVICES

The State may suspend, or terminate, or direct the Consultant to suspend or terminate, an End User's access to services in accordance with the State's policies an End User being an employee, subcontractor, or affiliate of Consultant. The State will assume sole responsibility for any claims made by End Users regarding the State's suspension/termination or directive to suspend/terminate such service. The Consultant may suspend access to services to an End User(s) immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of the Consultant's services or the network(s) or facilities used to provide the services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The Consultant may suspend access to services by an End User in response to a material breach by End User of any terms of use he or she has agreed to in connection with receiving the services. The Consultant will notify the State of any suspension of End User access to services.

## 9. SECURING OF DATA

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

## 10. USE OF PRODUCTION DATA IN A NON-PRODUCTION ENVIRONMENT

The Consultant cannot use protected State data, whether legally protected or protected by industry standards, in a non-production environment. Any non-production environment that is found to have legally protected production data~~,~~ must be purged immediately and the State Contact notified. The State will decide if this event is to be considered a security incident. "Legally protected production data" is any data protected under Federal or State Statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated or hashed is no longer considered to be legally protected.

## 11. MOVEMENT OF PROTECTED STATE DATA

The Consultant may not remove State data from the Salesforce system except with the express prior written consent of the State. To the extent State data is removed by Consultant, any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant's production or non-production systems, security must be maintained. The

Consultant will ensure that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP) referred to in paragraph 25 of this Exhibit, which are hereby incorporated by reference as part of this Exhibit.

## 12. BANNED SERVICES AND HARDWARE

The Consultant warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huwaei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, any subsidiary or affiliate of such entities, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

## 13. SECURITY INCIDENT NOTIFICATION

The Consultant will implement, maintain and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT ITSP or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The State requires notification of a Security Incident involving any of the State's sensitive data in the Consultant's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Consultant shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Consultant. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Consultant will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Consultant must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

A. The Consultant shall notify the State Contact within twelve (12) hours of the Consultant becoming aware that a Security Incident has occurred.

If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

C. At the State's discretion within twenty-four (24) hours the consultant must provide to the State all data available including: (i) Name of and contact information for the Consultant's Point of Contact for the Security Incident: (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered: (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred: and, (vii) the nature of the technologies involved. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person consultant must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Consultant shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Consultant is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Consultant reasonably determines that the breach will not likely result in harm to the affected person. The Consultant shall document the determination under this section in writing and maintain the documentation for

not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and consultant shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

14. HANDLING OF SECURITY INCIDENT

At the State's discretion the Consultant will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Consultant will also:

(i) fully investigate the incident,
(ii) cooperate fully with the State's investigation of, analysis of, and response to the incident,
(iii) make a best effort to implement necessary remedial measures as soon as it is possible and,
(iv) document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Consultant and at the Consultant's expense the Consultant will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Consultant shall offer three (3) years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Consultant, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense.

If the Consultant is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twelve (12) hours of the investigation report being completed. If the Consultant is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

15. SECURITY ACKNOWLEDGEMENT FORM

The Consultant will be required to sign a Security Acknowledgement form in a form acceptable to the State. This form constitutes the agreement of Consultant to be responsible and liable for ensuring that the Consultant's employee(s), and subcontractors, agents, assigns and/or affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP). Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Consultant does not sign another Security Acknowledgement form covering any employee(s) and any subcontractors, agents, assigns and/or affiliated entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Consultant's employee(s) or subcontractors, agents, assigns and/or affiliated entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Consultant or subcontractors, agents, assigns and/or affiliated entities and in accordance with the Consultant's or subcontractor's, agents, assigns and/or affiliated entities personnel policies. Regardless of the actions taken by the Consultant and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

## 16. BACKGROUND CHECKS

The State may at its option require all employee(s) of the Consultant, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. The State shall be responsible for costs associated with finger-print based background checks. These fingerprints will be used to check the criminal history records of both the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Consultant, subcontractors, agents, assigns and/or affiliated entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, subcontractors, agents, assigns and/or affiliated entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is

considered by the State to be a security risk, based on the results of the background check. The State will provide the Consultant with notice of this determination.

17. OFFSHORE SERVICES

The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

18. CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response.

19. DATA SANITIZATION

At the end of the project covered by this Agreement the Consultant, and Consultant's subcontractors, agents, assigns and/or affiliated entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Consultant and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Consultant will use a process and procedure that does satisfy the State.

20. CONFIDENTIALITY OF INFORMATION

For purposes of this paragraph, "State Proprietary Information" shall include all information disclosed to the Consultant by the State. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this agreement; (ii) make any use of State

Proprietary Information except to exercise rights and perform obligations under this agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or third party Consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this agreement. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in confidence at least equivalent with the standards employed in Consultant's industry. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities agree to return all information received from the State to State's custody upon the end of the term of this agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information shall not include information that:

(i) was in the public domain at the time it was disclosed to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities;
(ii) was known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction at the time of disclosure from the State;
(iii) that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;
(iv) was independently developed by the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without the benefit or influence of the State's information;
(v) becomes known to the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. Consultant acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

21. DATA RECOVERY

The Consultant must be able to recover the State's data in the same state it was sent to the Consultant. If the Consultant system or the third-party system that is hosting data for the Consultant is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the State data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the State and the Consultant.

## 22. REJECTION OR EJECTION OF CONSULTANT, AND CONSULTANT'S SUBCONTRACTORS, AGENTS, ASSIGNS AND/OR AFFILIATED ENTITIES EMPLOYEE(S)

The State, at its option, may require the vetting of any of the Consultant, and Consultant's Subcontractors, Agents, Assigns and/or Affiliated Entities. The Consultant is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Consultant to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Consultant with notice of its determination, and the reasons for the rejection or removal if requested by the Consultant. If the State signifies that a potential security violation exists with respect to the request, the Consultant shall immediately remove the individual from the project.

## 23. PROVISION OF DATA

Upon notice of termination by either party, the State will be provided by the Consultant all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Consultant with all current State Data in a non-proprietary form. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

## 24. ADVERSE EVENT

The Consultant shall notify the State Contact within two (2) days if the Consultant becomes aware that an Adverse Event has occurred. An Adverse Event is any of the following: the Consultant becoming aware of a credible security threat to its systems, unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Consultant's actions or inactions, the State can require a risk assessment of the Consultant the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Consultant's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

## 25. INFORMATION TECHNOLOGY STANDARDS

Any service, software or hardware provided under this agreement will comply with state standards which can be found at *http://bit.sd.gov/standards/* .

26. SECURITY

The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Consultant warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
   a. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
   b. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
   c. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
   d. **Low-** Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.

B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Consultant will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

C. The Consultant will fully support and maintain the Consultant's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Consultant may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Consultant's application to a new release of third-party technology if:
   i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
   ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Consultant may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.
If a code base or platform on which the Consultant's application depends is no longer supported, maintained, or patched by a qualified third party the Consultant commits to migrate its application from that code base and/or platform to one that is supported,

maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Consultant to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

27. MALICIOUS CODE

A. The Consultant warrants that the service contains no code that does not support an application requirement.
B. The Consultant warrants that the service contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the service or any media on which the service is delivered any malicious or intentionally destructive code.
D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the licensed software before installation. In the event any malicious code is discovered in the licensed software delivered by the Consultant, the Consultant shall provide the State at no charge with a copy of the applicable licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

28. LICENSE AGREEMENTS

Consultant warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end_users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

29. CONSULTANT TRAINING REQUIREMENTS

The Consultant, Consultant's employee(s), and Consultant's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response.

30. USE OF PORTABLE DEVICES

The Consultant shall prohibit its employees, agents, affiliates and subcontractors form storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Consultant's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

31. REMOTE ACCESS

The Consultant shall prohibit its employees, agents, affiliates and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

32. IN ALL INSTANCES IN WHICH GUIDEHOUSE MUST PROVIDE INFORMATION TO THE STATE ABOUT GUIDEHOUSE'S INFORMATION TECHNOLOGY INFRASTRUCTURE OR INFORMATION SECURITY POLICIES UNDER THIS SECTION, GUIDEHOUSE SHALL NOT BE REQUIRED TO DISCLOSE SUCH INFORMATION THAT GUIDEHOUSE REASONABLY DETERMINES WOULD COMPROMISE THE SECURITY OF GUIDEHOUSE TECHNOLOGY, NETWORKS, SYSTEMS, OR PREMISES OR THAT WOULD CAUSE GUIDEHOUSE TO ADVERSELY AFFECT OR BREACH ITS OBLIGATIONS OF CONFIDENTIALITY TO OTHER GUIDEHOUSE CLIENTS, PROVIDED THAT GUIDEHOUSE REASONABLY COOPERATES WITH THE STATE TO PROVIDE RESPONSIVE INFORMATION IN A MANNER THAT MINIMIZES OR AVOIDS GUIDEHOUSE SECURITY CONCERN.

AT THE STATE'S REQUEST, GUIDEHOUSE WILL PROVIDE THE STATE DOCUMENTARY EVIDENCE TO SUPPORT THE ASSERTION THAT GUIDEHOUSE MAINTAINS EFFECTIVE INTERNAL CONTROLS OVER INFORMATION SECURITY OF THE USE AND OPERATION OF THE TECHNOLOGY PLATFORM. GUIDEHOUSE AND THE STATE WILL COOPERATE TO DETERMINE AT THE TIME OF THE REQUEST THE SPECIFIC NATURE OF SUCH DOCUMENTATION.

## Exhibit A

## Task Order 1

Pursuant to Paragraph 1 of the Consulting Contract effective October 1, 2020, State issues the following Task Order for services under the Agreement:

### Scope of Work and Deadlines

Consultant shall provide the following deliverables:

1. End-to-End Grant Management and Process Design Services

   A. Consultant will:

   - Develop understanding of State's current grant processes and supporting cost/project management tools;
   - Begin preliminary design of a grant management process for State with respect to the following grant programs pursuant to the CARES Act:
     - Small business COVID interruption;
     - Small non-profit business COVID interruption;
     - Small business start-up;
     - Community-based health care providers or personal service providers;
     - Acute care in hospitals;
   - Establish the methodology and grants management system architecture to support the following:
     - Management of grant applications;
     - Eligibility verification;
     - Grant awards;
     - Management of grant agreements; and
     - Management of approval processes including the development of tracking and reporting mechanisms.

   B. Consultant shall begin work October 1 and deliver proposed solutions to State no later than October 13, 2020.

2. Grant Management Technology Platform Development

   A. Consultant will:

   - Implement and configure a Salesforce.com solution for grants management that:
     - Creates a seamless user experience;
     - Incorporates considerations and workflows around eligibility, application procedures, fraud, waste, and abuse identification;
     - Provides for dashboards and reporting;
     - Is provided via web portal and accessible to end-users via computer, tablet, or mobile phone;

- Incorporates federal guidelines and includes built-in checks to assist internal controls;
- Collects and makes available for extraction the data necessary for the State to issue payments and perform required federal reporting;

- Conduct testing, including developer testing and user acceptance testing (UAT) that:
  - Bundles completed work products into beta and production releases;
  - Includes the product owner and stakeholder team in interim demonstrations;
  - Performs continuous testing, verification, and validation;
  - Deploys releases incorporating such testing into the Staging/UAT environment;
  - Validates and smoke tests each build to ensure environmental continuity;
  - Performs a code quality and security analysis to ensure appropriate code standards are in place, where custom code is deemed necessary for the State of South Dakota.
- Trains users through "Train the Trainer" sessions with power users and TPA staff, in particular by:
  - Working closely with State support and development resources to facilitate knowledge-sharing;
  - Verifying that upon completion of the project, State has the confidence and capability to proceed with the new platform independent of significant outside assistance.

B. Consultant shall begin work October 1 and deliver a live, publicly accessible Salesforce.com solution for grants management to State no later than 8:00 a.m. CDT October 13, 2020. Additional testing, configuration adjustments, and training may take place after October 13, with final delivery and training completed by December 30, 2020.

3. Third Party Program Administration

A. Consultant will:

- Execute and operate the delivery model by:
  - Assisting the State in overseeing and validating applicant eligibility, expense categories and supporting documentation for each individual application;
  - Working closely with the State and applicants to coordinate the grant process, including developing and conducting preliminary scoring as determined during the design phase.
- Implement documentation management by:
  - Using the documentation management system to consolidate all:
    - Applicant eligibility documentation;

        - Any additional supporting documentation required for reimbursements as determined in the design phase;
    - Assisting the State and applicants in mapping the flow of documentation and requirements to ensure the compliant management of records.
- Develop reporting in order to ensure the following:
    - Executive-level reports that:
        - Track the disbursement of funds to ensure that they are being used as they were intended and in a timely fashion;
        - Identifies any potential risks and mitigation strategies;
        - Measures progress and ensures that taxpayer dollars are not only going where they were intended, but are also producing value and impact in the communities;
    - Assist the State in establishing a regular reporting schedule, gathering information, including by providing technical assistance, and performing a validation of information received.
- Provide technical assistance and subject matter expertise through guidance, support and communications around the following:
    - Applicant and eligibility reviews;
    - Providing cost eligibility guidelines to both South Dakota and applicants;
    - Access and usage of the grants portal (described in Section 2 of this Task Order);
    - Providing technical assistance and guidance on any ad-hoc issues;
    - Provide specialist/administrative support for review of funds (including any supporting documentation).

B. Consultant shall begin work no later than October 13, 2020 with final work completed by December 30, 2020.

4. Post-Funding Services

A. Consultant will:

- Develop, administer, and manage compliance reporting with the following components:
    - Identify Program Risks. Take inventory of known pitfalls and risks specific to the Small Business Grant Program of South Dakota
    - Prioritize and Evaluate. Prioritize risks based on vulnerability and impact
    - Respond and Manage. Develop a course of action for addressing the most significant risks to reduce risk exposure
    - Develop and Implement. Develop and implement a simplified compliance and monitoring effort

B. Consultant shall begin work no later than October 13, 2020 with final work completed by March 30, 2020.

BY: Liza Clark

Liza Clark
Commissioner
Bureau of Finance and
Management